REMARKS

This is in full and timely response to the Final Office Action of January 17, 2001. Reexamination in light of the amendments and the following remarks is respectfully requested.

Claims 1-39 are currently pending in this application, with claims 1, 2, 4, 5, 23, 24, 27 and 29 being independent.

No new matter is added.

The appreciation of the Applicant is expressed for the Examiner's helpful comments.

Claim objections

Claims 14 and 16-22 were objected to for various reasons.

In response, the claims have been amended exclusively for the purpose of correcting typographical errors.

Withdrawal of this objection is respectfully requested.

Rejection Under 35 USC 112

Claims 1-10, 13-22, 25-35 and 37 were rejected for various reasons under 35 USC 112.

While not conceding the propriety of these rejections, and in order to further the prosecution of the application, the claims have been amended.

Regarding the use of functional language, it is submitted that this usage is clear and definite, and that the use of functional language is proper. MPEP 2173.05(g).

Regarding the use of the terms "additional data", "various information", and "on the basis", "peculiar", and "similar", MPEP 2173.01 states that "a fundamental principle contained in 35 U.S.C. 112, second paragraph is that applicants are their own lexicographers. They can define in the claims what they regard as their invention essentially in whatever terms they choose so long as the terms are not used in ways that are contrary to accepted meanings in the art. Applicant may use functional language, alternative expressions, negative limitations, or any style of expression or format of claim which makes clear the boundaries of

the subject matter for which protection is sought. As noted by the Court in In re Swinehart, 439 F.2d 210, 160 USPQ 226 (CCPA 1971), a claim may not be rejected solely because of the type of language used to define the subject matter for which patent protection is sought."

Because these terms are not used in ways that are contrary to accepted meanings in the art, it is submitted that these terms are clear and definite, and that the use of these terms is proper.

Withdrawal of this rejection is respectfully requested.

Double Patenting Rejection

Claims 1-39 were rejected under the judicially created doctrine of obviousness-type double patenting as being allegedly unpatentable over claims 1-7 of U.S. Patent No. 5,933,625 issued to Sugiyama in view of U.S. Patent No. 5,502,765 issued Ishiguro et al. (Ishiguro) and the Examiner's Official Notice.

This rejection is respectfully traversed for at least the following reasons.

"There are some unique circumstances where it has been recognized that another type of nonstatutory double patenting rejection is applicable even where the inventions claimed in two or more applications/patents are considered nonobvious over each other." MPEP 804. However, in this type of double patenting rejection, "**only the claims** of the patent can be considered as support for the rejection, its disclosure being looked to only to determine the meaning of the claims, which are to be read in the light of the specification" (emphasis added). *id.*

"The Patent and Trademark Office (PTO) has the burden of showing a prima facie case of obviousness." *In re Bell*, 26 USPQ2d 1529, 1530 (Fed. Cir. 1993). "In determining the propriety of the Patent Office case for prima facie obviousness, it is necessary to ascertain whether the prior art teachings would appear to be sufficient to one of ordinary skill in the art to suggest making the proposed substitution or other modification." *In re Taborsky*, 183 USPQ 50, 55(CCPA 1974).

Although the Office Action states that Sugiyama does not teach of "time" renewal, the Office Action, nevertheless,

contends that "it would have been obvious to apply 'time' renewal means to the system and store these renewals in order further the life of the system and facilitate transactions whose life cycle extends beyond the initial fixed time period."

The Office Action further contends that "it would have been obvious to have the system's central, main, supervisor, managerial ... etc. computer to take on the role of 'official time-keeper'."

In response, these contentions are merely conclusory assertions that are unsupported by the cited prior art. Please note that the teachings, suggestions or incentives supporting the combination "must be clear and particular. Broad conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence.'" *In re Dembiczak*, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999).

The Office Action additionally states that Sugiyama "do not teach of registering means, appending new data to existing data, IC card applications, card verification, data collection, data updates and storage of time data."

The Office Action cites Ishiguro for some of the features deficient within Sugiyama.

Prima facie obviousness of a claimed invention is established "only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references." *In re Fine*, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

However, the Office Action fails to provide the proper motivation as to why the skilled artisan would have combined Ishiguro with Sugiyama for the features deficient within Sugiyama.

The Office Action states that Ishiguro does not specify any particular time keeping method.

Thus, there is an admission within the Office Action that not all features are taught by the combination of Ishiguro and Sugiyama.

The Office Action contends that "distributive business systems are 'well-known'" without providing a reference in support of this contention.

The Office Action further contends that "it is well-known" that the reduction in computing costs and the increase in processing speed has lead to a paradigm shift away from mainframes" without providing a reference in support of this contention.

The Office Actions states that neither Sugiyama nor Ishiguro detail the system in terms of specific commerce applications of an IC or smart card. Yet, the Office Action takes official notice that IC or smart cards that are used in electronic money applications or monetary transactions and that interact with gaming, banking or travel computers systems are well known in the art without providing a reference in support of this contention.

In response to these positions of Official Notice and what is well known, "it is facts which must support the legal conclusion of obviousness under 35 USC 103. Such facts must flow

from the prior art either by way of specific reference or by generally known facts of which official notice may be taken." *Ex parte Crissy et al.*, 201 USPQ 689, 695 (Bd. Pat. App. & Int. 1976). The specific reference or generally known facts must have existed "at the time the invention was made." *In re Merck & Co., Inc.*, 231 USPQ 375, 379 (Fed. Cir. 1986).

Further note that to support this officially noticed position of obviousness or what is well known, a reference, if in existence, or Examiner's affidavit is requested.

If this reference or Examiner's affidavit is not provided, the Official Notice or assertions of what is well known must be withdrawn. See MPEP 2144.03.

Although the Office Action rejects the claims as being doubly patented, the Office Action is replete with statements regarding what Sugiyama and Ishiguro fail to teach. The Office Action additionally makes unsupported references to what is well known.

Thus, a prima facie case of obviousness has not been established since each and every element as set forth in the claims are not found within Ishiguro, Sugiyama and the official notice.

Therefore, Ishiguro, Sugiyama and the official notice do not render obvious Applicant's invention. Furthermore, the claims are considered allowable for the reasons discussed above, as well as for the additional features they recite.

Withdrawal of this rejection is respectfully requested.

Conclusion

For the foregoing reasons, all the claims now pending in the present application are allowable, and the present application is in condition for allowance. Accordingly, favorable reexamination and reconsideration of the application in light of the amendments and remarks is courteously solicited.

If the Examiner has any comments or suggestions that could place this application in even better form, the Examiner is requested to telephone the undersigned attorney at the below-

listed number.

Respectfully submitted,

DATE: July 16, 2001

Brian K. Dutton
Reg. No. 47,255

RADER, FISHMAN & GRAUER PLLC
Lion Building
1233 20th Street, N.W.
Washington, D.C. 20036
Tel: (202) 955-3750
Fax: (202) 955-3751
Customer No. 23353

APPENDIX

IN THE CLAIMS:

Please amend the claims as follows.

1. An authentication-data issuing system based on unique time, said authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, said master computer comprising:

a unique time generating device including time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period;

transmitter means for, during communication between said master computer and another of the computers subservient to said master computer, transmitting, from said master computer to the subservient computer, authentication data based on an elapsed

time measurement, corresponding to a given time point, indicated by said unique time generating device; and

register means for receiving and registering an issuance history of unique authentication data created and issued by said subservient computer imparting additional data, unique to said subservient computer, to the authentication data transmitted by said master computer.

2. An authentication-data issuing system based on unique time, said authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, said master computer including a unique time generating device including time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period,

each of the computers subservient to said master computer comprising:

receiver means for, during communication with said master computer, receiving authentication data based on an elapsed time measurement, corresponding to a given time point, indicated by said unique time generating device of said master computer;

issuer means for creating and issuing unique authentication data by imparting additional data, unique to said subservient computer, to the authentication data received via said receiver means from said master computer; and

transmitter means for transmitting, to said master computer, an issuance history of the unique authentication data created and issued by said issuer means.

3. An authentication-data issuing system as recited in claim 2 wherein said issuer means in each of the subservient computers includes imparting means for imparting the additional data, unique to said subservient computer, to the received authentication data, and said imparting means includes a unique time generating device that includes time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially

accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period, and

wherein said unique time generating device in said imparting means indicates elapsed time measurements over the time-measuring period that is different from the time-measuring periods of the unique time generating devices provided in said master computer and other subservient computers and creates and issues unique authentication data peculiar to said subservient computer.

4. An authentication-data issuing system based on unique time, said authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, each of the computers subservient to said master computer comprising:

a unique time generating device including time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period unique to said computer that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by

said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period;

issuer means for creating and issuing unique authentication data, peculiar to said subservient computer, on the basis of an elapsed time measurement indicated by said unique time generating device; and

transmitter means for transmitting, to said master computer, an issuance history of the unique authentication data created and issued by said issuer means.

5. An authentication-data issuing system based on unique time, said authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, each of the computers subservient to said master computer comprising a unique time generating device including time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period unique to said computer that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by

said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period,

said master computer, exercising general control of the subservient computers, including register means for receiving and registering an issuance history of data created and issued by each of said subservient computers on the basis of an elapsed time measurement indicated by said unique time generating device of said subservient computer.

6. An authentication-data issuing system as recited in claim 3 wherein said master computer functions as an original supplier of unique time to said subservient computers so that said unique time generating devices of said subservient computers are activated to indicate elapsed time measurements within their respective preset time-measuring periods different from each other.

7. An authentication-data issuing system as recited in claim 3 wherein said master computer functions as an original supplier of unique time to said subservient computers so that said unique time generating devices of said subservient computers are activated to indicate elapsed time measurements within their

respective preset time-measuring periods different from each other, and each of the computers that are immediately subservient to said master computer is a second-level computer that functions as a secondary supplier of unique time data to third-level computers subservient to said second-level computer so that the unique time generating devices of said third-level computers are activated to indicate elapsed time measurements within their respective preset time-measuring periods different from each other.

8. An authentication-data issuing system as recited in claim 1 wherein said master computer includes storage means for storing data on said unique time generating device of each of the subservient computers which include data indicative of the time-measuring period of said unique time generating device, or

data on attributes of said unique time generating devices of said master computer and each of said subservient computers, or

unique additional data to be imparted, by each of said subservient computers, to the authentication data received from said master computer.

9. An authentication-data issuing system as recited in claim 1 wherein the unique authentication data created and issued by each of said subservient computers is transmitted to and used by one or more other subservient computers under control of said master computer every time a transaction involving use of the unique authentication data is performed.

10. An authentication-data issuing system as recited in claim 1 wherein the unique authentication data created and issued by each of said subservient computers includes various information to be transmitted to one or more other subservient computers under control of said master computer, said various information including any of information representative of nature of a transaction, merchandise, settlement of account and credit standing.

11. A recording media having stored thereon unique authentication data created by any one of said subservient computers as recited in claim 1, said recording media being issued by said subservient computer.

12. A recording media as recited in claim 11 which comprises a floppy disk, IC card, magnetic card or writable CD-ROM.

13. A recording media as recited in claim 11 where the unique authentication data stored thereon includes any of monetary information, information on credit loan, money information indicative of a current balance of deposit or saving in a particular account, and information indicative of permission or refusal of use of an amusement part, game house, recreational facility, a railroad, bus, ship, airplane, telephone, facsimile, automatic vending machine or the like.

14. (amended) An authentication-data issuing system as recited in claim 1 wherein said master computer is a host computer of a central bank exercising general control of banking operations and said subservient computers are computers of banking agencies [such as] including city banks, local banks and credit banks under control of the host computer of the central bank, and wherein a transaction[, such as] including money supply, settlement, loaning, money changing or payment into account, between any one of the banking agencies and a customer is

performed on the basis of unique authentication data created and issued for each transaction.

15. (amended) An authentication-data issuing system as recited in claim 1 wherein said master computer is a host computer of a main office of a banking agency exercising general control of a plurality of branches, local offices and the like of the banking agency and said subservient computers are computers installed in the main office, branches and local offices of the banking agency, and wherein a transaction[, such as] <u>including</u> money supply, settlement, loaning, money changing or payment into account, between any one of the subservient computers and a customer is performed on the basis of unique authentication data created and issued for each transaction.

16. (amended) An authentication-data issuing system as recited in claim 1 wherein said mater computer is a host computer of a main office exercising general control of an organization [such as] <u>including</u> a company or corporation and said subservient computers are computers for use at various stations or by constituent members of the organization, and wherein an operation to be effected by each of the stations or constituent members is

performed on the basis of unique authentication data created and issued by the corresponding subservient computer for each operation.

17. An authentication-data issuing system as recited in claim 1 wherein said mater computer is a host computer of an administrative organ exercising general control of administrative affairs and said subservient computers are computers for use at various stations or by constituent members of the administrative organ, and wherein an operation to be effected by each of the stations or constituent members is performed on the basis of unique authentication data created and issued by the corresponding subservient computer for each operation.

18. (amended) A recording media as recited in claim 11 wherein said mater computer is a host computer of a transportation company exercising general control of operations for issuing various tickets[, such as] <u>including</u> an ordinary passenger ticket, railroad and ship tickets, coupon ticket, commuter pass and airline ticket and said subservient computers are computers contained in vending machines installed in a station, airlines, shipping company, tourist bureau, convenience store and the like,

said recording media being employed as the [thicket] ticket issued by any one of the vending machines and having stored thereon unique authentication data that is created by said subservient computer of the vending machine every time the ticket is used.

19. A recording media as recited in claim 11 wherein said mater computer is a host computer exercising general control of operations for issuing various prepaid cards for using a railroad, ship, airplane, pachinko game machine, telephone, amusement park and the like and said subservient computers are computers contained in vending machines for issuing the prepaid cards, said recording media being employed as the prepaid card issued by any one of the vending machines and having stored thereon unique authentication data that is created by said subservient computer of the vending machine every time the ticket is used.

20. (amended) A recording media as recited in claim 11 wherein said mater computer is a host computer of a central bank exercising general control of operations for issuing electronic money and said subservient computers are computers contained in

money issuing machines for issuing electronic money to users, said recording media being employed as the electronic money issued by any one of the money issuing machines and having stored thereon unique authentication data that is created by said subservient computer of the money issuing machine every time the electronic money is used.

21. (amended) A recording media as recited in claim 11 wherein said mater computer is a host computer of an administrative organ exercising general control of public services to be provided to individual residents and said subservient computers are computers contained in card issuing machines for issuing personalized ID cards that are to be used by the individual residents to get the public services, said recording media being employed as the ID card issued by any one of the card issuing machines and having stored thereon unique authentication data that is created by said subservient computer of the vending machine every time the ID card is used.

22. (amended) A recording media as recited in claim 11 wherein said mater computer is a host computer exercising general control of operations of a banking agency, credit company, securities

company, insurance company, loan company and trust company issuing cards [such as] including a cash card, loan card and credit card and said subservient computers are computers contained in card issuing machines for issuing cards to individual customers, and which is employed as said card issued by any one of the card issuing machines and has stored thereon in magnetic form unique authentication data that is created by said subservient computer of the money issuing machine every time the card is used.

23. An authentication-data verifying system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, each of the computers subservient to said master computer comprising:

reading means for reading unique authentication data issued by any one of the subservient computers on the basis of information received from another of the subservient computers, or reading unique authentication data issued by any one of the subservient computers and recorded on a recording media;

transmitter means for transmitting the unique authentication data read by said reading means to said master computer for subsequent collation thereby; and

receiver means for receiving from said master computer a result of collation between an issuance history of the unique authentication data by each of said subservient computers registered in said master computer and the unique authentication data transmitted by said transmitter means.

24. An authentication-data verifying system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, said master computer comprising:

receiver means for receiving unique authentication data transmitted by transmitter means of any one of the computers subservient to said master computer, said unique authentication data being issued by the subservient computer and read by reading means of the subservient computer; and

collator means for collating between the unique authentication data received by said receiver means and an issuance history of the unique authentication data by each of

said subservient computers that is registered in said master computer; and

transmitter means for transmitting a result of collation by said collator means to receiver means of the subservient computer.

25. An authentication-data verifying system as recited in claim 23 wherein each of said subservient computers includes rejecting means which when a result of the collation by said collator means of said master computer indicates that the unique authentication data read by said reading means is not present in the issuance history, rejects subsequent access between said subservient computer and another of said subservient computers or rejects use, in said subservient computer, of a recording media having stored thereon the unique authentication data.

26. An authentication-data verifying system as recited in claim 23 wherein each of said subservient computers includes authorizing means which when a result of the collation by said collator means of said master computer indicates that the unique authentication data read by said reading means is present in the issuance history, authorizes subsequent access between said

subservient computer and another of said subservient computers or authorizes use, in said subservient computer, of a recording media having stored thereon the unique authentication data.

27. An authentication-data issuing system based on unique time, said authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, each of the computers subservient to said master computer being accessed by another of the subservient computers on the basis of unique authentication data authorized by said authorizing means recited in claim 26 or being connected with a recording media, having stored thereon the unique authentication data whose use is permitted by said authorizing means recited in claim 26,

said master computer comprising a unique time generating device including time keeping means provided in said master computer for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by said

time keeping means so as to constantly measure a changing elapsed time within the time-measuring period,

each of said subservient computers comprising: receiver means for, during communication with said master computer, receiving authentication data based on an elapsed time measurement, corresponding to a given time point, indicated by said unique time generating device;

issuer means for creating and issuing unique authentication data by imparting additional data, unique to said subservient computer, to the authentication data received via said receiver means; and

transmitter means for transmitting, to said master computer, the unique authentication data created and issued by said issuer means.

28. An authentication-data issuing system as recited in claim 27 wherein said issuer means in each of said subservient computers includes imparting means for imparting, to the received authentication data, the additional data unique to said subservient computer, and said imparting means includes a unique time generating device that includes time keeping means for sequentially outputting unit time values at predetermined

intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period, and

wherein said unique time generating device in said imparting means indicates elapsed time measurements over a time-measuring period that is different from time-measuring periods of the unique time generating devices provided in said master computer and other subservient computers and creates and issues unique authentication data peculiar to said subservient computer.

29. An authentication-data issuing system based on unique time, said authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, each of the computers subservient to said master computer being accessed by another of the subservient computers on the basis of unique authentication data authorized by said authorizing means recited in claim 26 or being connected with a recording media,

having stored thereon unique authentication data whose use is authorized by said authorizing means recited in claim 26,

each of said subservient computers comprising:

a unique time generating device for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period;

issuer means for creating and issuing unique-authentication-data updating data, corresponding to the authorized unique authentication data, on the basis of an elapsed time measurement indicated by said unique time generating device; and

transmitter means for transmitting, to said master computer, the unique-authentication-data updating created and issued by said issuer means.

30. An authentication-data issuing system based on unique time, said authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, each

of the computers subservient to said master computer being accessed by another of the subservient computers on the basis of unique authentication data authorized by said authorizing means recited in claim 26 or being connected with a recording media, having stored thereon unique authentication data whose use is authorized by said authorizing means recited in claim 26,

said master computer comprising:

a unique time generating device including time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and accumulating means for sequentially accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period;

transmitter means for transmitting to, any one of the subservient computers, authentication data based on an elapsed time measurement, corresponding to a given time point, indicated by said unique time generating device; and

renewal means for receiving unique-authentication-data updating data that is created and issued by the subservient computer imparting additional data, unique to the subservient

computer, to the authentication data from said transmitter means of said master computer, and altering the unique authentication data on the basis of the received unique-authentication-data updating data to thereby update an issuance history of the unique authentication data by said subservient computer that is registered in said master computer.

31. An authentication-data issuing system based on unique time, said authentication-data issuing system including a plurality of computers connected with each other via communication lines with one of said computers set to function as a master computer, each of the computers subservient to said master computer being accessed by another of the subservient computers on the basis of unique authentication data permitted by said authorizing means recited in claim 26 or being connected with a recording media, having stored thereon the unique authentication data whose use is permitted by said authorizing means recited in claim 26,

said subservient computer including a unique time generating device which includes time keeping means for sequentially outputting unit time values at predetermined intervals over a preset time-measuring period that begins at a given start point on a selected date and terminates at a given future end point and

accumulating means for sequentially accumulating said unit time values output by said time keeping means so as to constantly measure a changing elapsed time within the time-measuring period,

said master computer including renewal means for receiving unique-authentication-data updating data that is created and issued by the subservient computer in correspondence with the authorized unique authentication data and altering the unique authentication data on the basis of the received unique-authentication-data updating data to thereby update an issuance history of the unique authentication data by said subservient computer that is registered in said master computer.

32. (amended) An authentication-data issuing system as recited in claim 30 wherein said subservient computer includes renewal means[, similar to said renewal means of said master computer,] for altering the unique authentication data used [for] to gain[ing] authorization to access [to] another of the computers or to make use of the recording media, on the basis of the unique-authentication-data updating data.

33. (amended) An authentication-data issuing system as recited in claim 32 wherein said renewal means of said subservient computer

receives data relating to the issuance history updated by said renewal means of said master computer, [in such a way that] said subservient computer updat<u>ing</u>[es] the unique authentication data on the basis of the received data relating to the issuance history.

34. An authentication-data issuing system as recited in claim 32 wherein the unique authentication data updated by said renewal means is stored in memory of the subservient computer, having accessed using last-issued unique authentication data, so that the updated unique authentication data is used for next access to another of the subservient computers.

35. An authentication-data issuing system as recited in claim 32 wherein said renewal means alters last-issued unique authentication data, stored on the recording media used in said subservient computer, on the basis of the created and issued unique-authentication-data updating data.

36. An authentication-data issuing system as recited in claim 14 wherein the unique authentication data created and issued by

said subservient computer contains the unique authentication data updated by renewal means.

37. A recording media having stored thereon unique authentication data updated by the unique-authentication-data updating data created and issued in claim 35.

38. An authentication-data issuing system as recited in claim 37 wherein the recording media having stored thereon updated unique authentication data is a ticket, a prepaid card, an electronic money, an ID card, or a card, and wherein the subservient computer that stores the updated unique authentication data on said recording media is contained in or attached to an automatic ticket checker or a card reader/writer for the prepaid card, the ID card or the electronic money.

39. An authentication-data issuing system based on unique time or recording media issued by said authentication-data issuing system as recited in claim 38 wherein the recording media used in said subservient computer is a ticket, electronic money, prepaid card or other card, and wherein information indicative of a current balance calculated by subtracting, from a money amount

stored on said recording media, a money amount spent at the time of creation of the updated unique authentication data.